UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/581,496	06/27/2007	Karthik Kaleedhass	3587-0124PUS1	3830

2292 7590 08/23/2010

BIRCH STEWART KOLASCH & BIRCH
PO BOX 747
FALLS CHURCH, VA 22040-0747

EXAMINER	
LEWIS, LISA C	

ART UNIT	PAPER NUMBER
2436	

NOTIFICATION DATE	DELIVERY MODE
08/23/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

mailroom@bskb.com

Office Action Summary	Application No.	Applicant(s)	
	10/581,496	KALEEDHASS ET AL.	
	Examiner	Art Unit	
	Lisa Lewis	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 June 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *02 June 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-24 are presented for examination on the merits.

Claim Rejections - 35 USC § 112

1. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claims 1-24 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

3. The claims are vague and indefinite because they contain numerous grammatical errors. For example, claim 5 recites: "as claimed in claim 3, wherein upon detecting a failure in the first attempt claim 4 the access apparatus..." The claim dependency and the claim language itself are unclear. (Claim 8 is rejected similarly). Claim 7 recites "imputing" instead of "inputting". Claim 15 recites "a transmission means wherein the encrypted biometric **features** of the individual **is** transmitted." Claims 22-24 recite "an electronic means of identifying…as claimed in claim 1". However, claim 1 is a method. Additional grammatical mistakes may be in the claims and a thorough review and correction of all claims is required for clarity.

4. Further, in claim 1, the term "the biometric features" lacks sufficient antecedent basis and it is unclear whether there is one feature or multiple features.

5. Regarding claim 1, the phrase "such as" renders the claim indefinite because it is unclear whether the limitations following the phrase are part of the claimed invention. See MPEP § 2173.05(d).

6. Regarding claim 10, the limitation "the server is provided in storage medium including a token" is unclear. How can a server collecting and storing biometric data and verification information, and making verification decisions be implemented on a token? Perhaps claim should recite, "the server is

provided on a storage device capable of recording data", or "the apparatus is provided in a storage medium including a token..." Appropriate clarification is required.

7. All other claims depend directly or indirectly from the above claims, and are therefore also rejected under 35 U.S.C. 112 2nd paragraph.

Claim Rejections - 35 USC § 102/103

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 1-4, 10, 11, 13-20, 23, and 24 are rejected under 35 U.S.C. 102(e) as being anticipated by, or in the alternative, under 35 U.S.C. 103(a), as being unpatentable over Uchida (US 7,246,243).

11. Regarding claims 1 and 10, Uchida teaches a method of electronically identifying and verifying an individual utilizing at least one biometric feature of the individual including the steps of:

a. Activating an access apparatus (capable of recording data - see 112 2nd paragraph rejection with regards to claim 10) with a means to capture at least one biometric feature of an individual in a secure manner using dynamic encryption (A user's fingerprint is detected by a fingerprint sensor and is encrypted) - see figure 13 and column 3 line 64 - column 4 line 18, for example.

b. Capturing the biometric feature of an individual wherein key feature of biometric raw data are extracted (A user's fingerprint is captured, and features, such as ridge patterns, of the fingerprint are extracted) - see figure 13 and column 3 line 64 - column 4 line 18, for example.

c. Encrypting in a dynamic manner the biometric features (The features are encrypted using a secret key generated by a cipher key generator) - see figure 13 and column 3 line 64 - column 4 line 18, for example.

d. Transmitting the encrypted data of the biometric feature to at least one server (The encrypted data is transmitted to an authentication server) - see figure 13, column 2 lines 39-57, and column 3 line 64 - column 4 line 18, for example.

e. Verifying the biometric features captured with a pre-stored biometric feature in the server (It is determined whether the received biometrics data has corresponding biometrics data in the database for authentication) - see figure 13, column 5 lines 36-52, column 2 lines 39-57, and column 3 line 64 - column 4 line 18, for example.

i. Wherein upon positive identification and verification of the individual access is given to an auxiliary means such as but not limited to access to secured doors, database, computer network, or servers (Access is given to e-commerce over a communications network if the biometric matches a biometric associated with an ID in the database) - see column 1 and column 5 lines 4-16, for example.

12. Regarding claim 15, Uchida teaches an electronic means of identifying and verifying an individual presenting for such identification and verification including:

f. A means to capture at least one type of biometric features of the individual (A user's fingerprint is detected by a fingerprint sensor and features are extracted) - see figure 13 and column 3 line 64 - column 4 line 18, for example.

g. A software means to encrypt in a dynamic manner the biometric features (The features are encrypted using a secret key generated by a cipher key generator) - see figure 13 and column 3 line 64 - column 4 line 18, for example.

h. A transmission means wherein the encrypted biometric features of the individual are transmitted to a server (The encrypted data is transmitted to an authentication server) - see figure 13, column 2 lines 39-57, and column 3 line 64 - column 4 line 18, for example.

i. A software means to capture the encrypted biometric features presented for identification and verification against stored encrypted biometric features of a purported individual (It is determined whether the received biometrics data has corresponding biometrics data in the database for authentication and identification (A user's identifier ID-A is compared)) - see figure 13, column 5 lines 36-52, column 2 lines 39-57, column 5 lines 4-16, and column 3 line 64 - column 4 line 18, for example.

j. A means to give access to other databases or software if a positive identification and verification is made and to deny such access if a negative identification and verification is made (Access is given to e-commerce over a communications network if the biometric matches a biometric associated with an ID in the database. Denial or authorization is given based on the match) - see column 1, figure 11, and column 5 lines 4-16, for example. Please note that this would inherently require access to some type of software and/or database.

13. Regarding claim 19, Uchida teaches an electronic means of identifying and verifying an individual presenting for such identification and verification including:

k. Access apparatus with a means to capture at least one biometric raw data of an individual in a secure manner using dynamic encryption (A user's fingerprint is detected by a fingerprint sensor and is encrypted) - see figure 13 and column 3 line 64 - column 4 line 18, for example.

l. Circuitry to extract any features of the biometric raw data from the means to capture the biometric raw data (A user's fingerprint is captured, and features, such as ridge patterns, of the fingerprint are extracted) - see figure 13 and column 3 line 64 - column 4 line 18, for example.

m. Circuitry to encrypt the key features of the biometric raw data in a dynamic manner (The features are encrypted using a secret key generated by a cipher key generator) - see figure 13 and column 3 line 64 - column 4 line 18, for example.

n. Transmission means to transmit encrypted data of the biometric features to at least one server (The encrypted data is transmitted to an authentication server) - see figure 13, column 2 lines 39-57, and column 3 line 64 - column 4 line 18, for example.

o. At least one server to receive and store the encrypted data of the biometric feature of the individual (The authentication server stores the received data) - see figure 13, column 2 lines 39-57, and column 3 line 64 - column 4 line 18, for example.

p. Circuitry to verify and/or identify the encrypted data against pre-stored encrypted biometric data in the server (It is determined whether the received biometrics data has corresponding biometrics data in the database for authentication and identification (A user's identifier ID-A is compared)) - see figure 13, column 5 lines 36-52, column 2 lines 39-57, column 5 lines 4-16, and column 3 line 64 - column 4 line 18, for example.

14. Regarding claims 2-4 and 20, Uchida teaches that the server is spatially separated from access apparatus - see figure 13 and column 2 lines 39-56, for example.

15. Regarding claims 11, 16, and 24, Uchida teaches comparing the biometric features with known biometric features from a database and by a PIN (ID) - see - see figure 13, column 5 lines 36-52, column 2 lines 39-57, column 5 lines 4-16, and column 3 line 64 - column 4 line 18, for example.

16. Regarding claims 13, 14, and 23, Uchida teaches that the features are stored at the server itself - see figure 13 and column 2 lines 39-56, for example.

17. Regarding claims 17 and 18, Uchida teaches that the biometric is a fingerprint - see - see figure 13 and column 3 line 64 - column 4 line 18, for example.

18. Therefore, it appears that the teachings of Uchida anticipate the limitations of claims 1-4, 10, 11, 13-20, 23, and 24. In the alternative, even if the claimed invention is not identical to that disclosed by the cited reference (e.g., if there is no access to a particular software, per se), the differences between that which is disclosed and that which is claimed are considered to be so slight that that it would have been obvious to the skilled artisan to modify the teachings of Uchida in order to create the claimed invention.

19. Accordingly, the claimed invention as a whole was at least prima facie obvious, if not anticipated by the reference, especially in the absence of sufficient, clear, and convincing evidence to the contrary.

Claim Rejections - 35 USC § 103

20. Claims 7, 8, and 12 are rejected under 35 U.S.C. 35 U.S.C. 103(a) as being unpatentable over Uchida (US 7,246,243).

21. Regarding claim 7, Uchida further teaches that registration is performed into a database by a user supplying their fingerprint and ID to the machine, which is sent to the authentication server for registration i.packet, and the data is stored in the server - see column 4 line 56 - column 5 line 3 and column 5 lines 17-24, for example. Uchida does not expressly teach that the data features are encrypted or that the step is performed before a user inputs their biometric feature for authorization. However, for basic security purposes, and to maintain uniformity throughout the system, the skilled artisan would recognize that it is the intention of Uchida that the features be extracted and encrypted. Further, collecting registration information first and in a separate step, is merely a matter of design choice and does not affect patentability.

22. Regarding claim 8, Uchida teaches that the particulars are an ID (alpha numeral) - see column 4 line 56 - column 5 line 3 and column 5 lines 17-24, for example.

23. Regarding claim 12, using or eliminating the PIN or user ID is merely a matter of design choice based on security preferences, and is well within the purview of the skilled artisan to discern.

24. Claims 5, 6, 21, and 25 are rejected under 35 U.S.C. 35 U.S.C. 103(a) as being unpatentable over Uchida in view of Bianco et al. (US 6,256,737).

25. The teachings of Uchida are relied upon for the reasons set forth above.

26. Regarding claims 5, 21, and 25, Uchida does not teach a backup server that the data is rerouted to in a case of failure.

27. Bianco et al. beneficially teach that an alternate biometric server is used as a backup server to biometric data and stores the exact same data so that a server is always available to authenticate users - see column 10 lines 28-35, for example.

28. It would have been obvious to one of ordinary skill in the art at to create the invention as claimed for the following reasons. It would have been obvious to one of ordinary skill in the art at the time the claimed invention was made to modify the teachings of Uchida by allowing a backup server to be available in the event of failure, for the purpose of making authentication always available to users, based upon the beneficial teachings provided by Bianco et al. These modifications would result in increased security and efficiency, both of which are obvious benefits to the skilled artisan. Additionally, the cited references are in the field of biometric authentication, as is the current application, and thus, are in analogous arts.

29. Regarding claim 6, Uchida teaches that the server is spatially separated from access apparatus - see figure 13 and column 2 lines 39-56, for example.

30. Claim 9 is rejected under 35 U.S.C. 35 U.S.C. 103(a) as being unpatentable over Uchida in view of McCabe (US 2002/0095317).

31. The teachings of Uchida are relied upon for the reasons set forth above.

32. Regarding claim 9, Uchida does not teach that the sever is located in a separate country.

33. McCabe beneficially teaches that two backup servers should be used and that one can be located on the opposite end of the country and the other can be located on a different continent - see [0109], for example.

34. It would have been obvious to one of ordinary skill in the art at to create the invention as claimed for the following reasons. It would have been obvious to one of ordinary skill in the art at the time the

claimed invention was made to modify the teachings of Uchida by allowing the server to reside on another country, for the purpose of increased security, based upon the beneficial teachings provided by McCabe. Additionally, the cited references are in the field of computer security, as is the current application, and thus, are in analogous arts.

35. Claim 22 is rejected under 35 U.S.C. 35 U.S.C. 103(a) as being unpatentable over Uchida in view of Robinson et al. (US 2008/0271116).

36. The teachings of Uchida are relied upon for the reasons set forth above.

37. Regarding claim 22, Uchida does not teach that a token is used in addition to the biometric sample.

38. Robinson et al. beneficially teach that in addition to a biometric sample, a token with identification information can be presented for identification verification - see [0049], for example.

39. It would have been obvious to one of ordinary skill in the art at to create the invention as claimed for the following reasons. It would have been obvious to one of ordinary skill in the art at the time the claimed invention was made to modify the teachings of Uchida by allowing a token to be used in addition to the biometrics, for the purpose of increased security and ease of use, based upon the beneficial teachings provided by Robinson et al. Additionally, the cited references are in the field of biometrics, as is the current application, and thus, are in analogous arts.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Lisa Lewis whose telephone number is (571) 270-7724. The examiner can normally be reached on Monday - Friday, 6:30 a.m. - 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Nasser Moazzami/
Supervisory Patent Examiner, Art Unit 2436

/L. L./
Examiner, Art Unit 2436